UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

ROBERT CRIST and REBECCA L. LEMMONS, individually and on behalf of those similarly situated, Plaintiffs, v. **EISNERAMPER LLP and EISNER ADVISORY GROUP LLC**, Defendants.	Case No. 25-cv-1573 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Robert Crist and Rebecca L. Lemmons ("Plaintiffs") brings this Class Action Complaint ("Complaint"), on behalf of themselves and all others similarly situated, against Defendants EisnerAmper LLP and Eisner Advisory Group LLC (collectively "Eisner" or "Defendant") for failure to properly secure and safeguard Plaintiffs' and Class members' personally identifiable information ("PII") stored within Defendant's information network and alleging as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which is based on personal knowledge:

NATURE OF THE CASE

1. Entities that provide services and handle customers and employees' sensitive PII owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII to unauthorized persons—especially hackers with

nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private financial matters.

2. The harm resulting from a breach of private data manifests in a number of ways, including identity theft and financial fraud. The exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and to take a number of additional prophylactic measures.

3. As a provider of accounting and tax advisory services, Eisner knowingly obtains sensitive customer and employee PII and has a resulting duty to securely maintain such information in confidence.

4. As discussed in more detail below, Eisner breached its duty to protect the sensitive PII entrusted to it. As such, Plaintiffs bring this Class action on behalf of themselves and other individuals whose PII was accessed and exposed to unauthorized third parties during a data breach of Defendant's system which was announced when Eisner posted a notice on its website[1] and began mailing out notices to affected individuals on or about April 8, 2025. (the "Data Breach").

[1] https://www.eisneramper.com/globalassets/pdfs/eisner_website-notice_with-hotline.pdf (last visited April 16, 2025).

5. According to internet news sources, between September 4 and September 9, 2023, a well-known ransomware group accessed Defendant's information network and exfiltrated a massive amount of data from Defendant's network.[2] While Eisner has offices across the country and is headquartered in New York, it has publicly identified the Minneapolis office as being the source of the Data Breach.[3] However, Defendant has failed to disclose the nature of the attack.[4] According to information Defendant provided to the Maine Attorney General, the breach affected approximately 85,000 individuals' PII.[5]

6. The data stolen included Plaintiffs' and Class members' PII, including customers' names, contact information, date of birth, credit card information, driver's license information, and Social Security numbers.[6]

7. As a direct and proximate result of Eisner's inadequate data security and its breach of its duty to handle PII with reasonable care, Plaintiffs' PII has been accessed by hackers, potentially posted on the dark web, and exposed to an untold number of unauthorized individuals.

---

[2] https://beyondmachines.net/event_details/eisner-advisory-group-reports-data-breach-i-6-n-q-7/gD2P6Ple2L (last visited April 16, 2025).

[3] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/602a61a2-18b4-4e62-be78-93cfe3ef3653.html (last visited April 16, 2025).

[4] https://beyondmachines.net/event_details/eisner-advisory-group-reports-data-breach-i-6-n-q-7/gD2P6Ple2L

[5] *See* Maine Attorney General Data Breach Notification, attached as Exhibit A.

[6] *Id*.

8. Plaintiffs are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, and such risks may last for the rest of their lives. Consequently, Plaintiffs must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. Plaintiffs, on behalf of themselves and others similarly situated, brings claims for negligence, breach of a third party contract, breach of fiduciary duty, breach of confidences, unjust enrichment, and declaratory judgment; seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

10. To recover from Eisner for their sustained, ongoing, and future harms, Plaintiffs and Class members seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendant to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

Plaintiffs

11. Plaintiff Robert Crist is an adult individual and, at all relevant times herein, was a resident and citizen of California. On or about April 8, 2025, Plaintiff Crist was notified of the Data Breach and of the impact to his PII via letter from Defendant.

12. Plaintiff Rebecca L. Lemmons is an adult individual and, at all relevant times herein, a resident and citizen of Florida. Some time prior to September 2023, Plaintiff Lemmons obtained accounting and tax advisory services through an accountant that utilizes the Eisner network and, therefore, is an Eisner customer and a victim of the Data Breach. On or about April 8, 2025 Plaintiff was notified of the Data Breach and of the impact to her PII via letter from Defendant.

13. As a result of Defendant's conduct, Plaintiffs suffered actual damages including, without limitation, time related to monitoring their financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm. Plaintiffs and Class members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

Defendants EisnerAmper LLP and Eisner Advisory Group LLC

14. Defendant EisnerAmper LLP is a licensed independent CPA firm that provides accounting and tax advisory services and maintains office throughout the United States and internationally with more than 450 partners and 4,500 employees.[7] Eisner maintains its headquarters at 733 Third Avenue, New York, NY and its regional headquarters at 2780 Snelling Avenue N, Suite 101, Roseville, MN 55113.

[7] https://www.linkedin.com/company/eisneramper/about/ (last visited April 16, 2025)

15. Defendant Eisner Advisory Group LLC is a New York limited liability company operating under the Eisner Advisory Group LLC umbrella that provides tax and business consulting services to its clients.[8] It maintains its headquarters at 733 Third Avenue, New York, NY and its regional headquarters at 2780 Snelling Avenue N, Suite 101, Roseville, MN 55113.

16. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiffs.

17. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's states of citizenship.

19. This Court has personal jurisdiction over the parties in this case. Defendant Eisner conducts business in this District and is a citizen of this District by virtue of having a principal place of business located in this District.

20. Venue is proper in this District under 28 U.S.C. §1391(b) because Eisner maintains a headquarters in this District and regularly conducts business in this District.

[8] https://www.eisneramper.com/ (last visited April 16, 2025).

FACTUAL BACKGROUND

A. Eisner and the Services it Provides.

21. Eisner "offers businesses, government organizations, and individuals a comprehensive set of accounting and audit, tax, advisory, and outsourcing services to help them respond quickly to urgent issues, anticipate opportunities and risks, and grow profitably."[9]

22. While administering its accounting and tax advisory services, Eisner receives and handles PII, which includes, *inter alia*, customer and employees' full name, address, Social Security number, driver's license or state ID number, financial account and payment card information.

23. By obtaining, collecting, and storing Plaintiffs' PII, Eisner assumed legal and equitable duties and knew or should have known that Defendant was responsible for protecting Plaintiffs' PII from unauthorized disclosure.

24. And, upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class members to entities that retain Eisner.

B. Eisner Knew the Risks of Storing Valuable PII and the Foreseeable Harm to its Customers and Employees.

25. At all relevant times, Eisner knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

[9] https://www.eisneramper.com/about-us/global-reach/ (last visited April 16, 2025).

26. Eisner also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private information.

27. In fact, during June 2023, Eisner published a white paper for its clients educating them on how to avoid data breaches, noting that "[t]he good news is that there are many simple steps you can take to prevent hackers from accessing your vital business data."[10]

28. Eisner instructs its clients to:

> Take Preemptive Action
>
> You will significantly decrease the likelihood of having to deal with a business data breach if you take the right actions to prevent this from happening. Here are the most important things that you should consider in preparation.
>
> Conduct a Risk Assessment
>
> Understanding your vulnerabilities is key to creating a robust data breach response plan. A risk assessment helps you identify potential weak points in your digital infrastructure.[11]

29. Moreover, Eisner should have been aware that accounting, tax, and business advisory firms have become prime targets for cybercriminals, and thus alerted to its

[10] https://www.eisneramper.com/insights/outsourced-it/data-breach-response-0623/ (last visited April 16, 2025).

[11] *Id.*

susceptibility to cyberattack and taken proactive measures to enhance its data security.[12] An article in the Kansas City Star reports "[h]ackers focus on financial services because these firms store valuable client data, including financial information and personally identifiable information. Cybercriminals exploit gaps in security to steal this data for identity theft, fraud, or sale on the dark web."[13]

30. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[14]

31. For example, in 2023, the number of data compromises in the United States stood at 3,205 cases, affecting over 353 million individuals.[15]

32. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's customers and employees especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank

---

[12] https://www.kansascity.com/news/business/personal-finance/article299479089.html (last visited April 16, 2025).

[13] *Id.*

[14] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[15] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last visited April 16, 2025).

fraud, and more.

33. PII is a valuable property right.[16] The value of PII as a commodity is measurable.[17] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[18] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[19] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" or the "dark web," for many years.

34. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the

---

[16] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

[17] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle./824192.

[18] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[19] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

35. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[20]

36. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

37. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and

[20] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited April 16, 2025).

accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[21]

38. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

39. Based on the value of its customers' and employees' PII to cybercriminals and cybercriminals' propensity to target businesses, Eisner certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. **Eisner Breached its Duty to Protect its Customers and Employees PII.**

40. On or about April 8, 2025, Eisner announced that it experienced a security incident disrupting access to its systems. As above, the breach occurred when CLOP, a well-known ransomware group, stole massive amounts of data and encrypted Eisner's information network, making it inaccessible and unusable by Eisner's employees.[22]

41. Presently, however, Defendant has provided no public information on the ransom demand or payment. Additionally, Eisner failed to explain why it waited for nearly 18 months after the initial breach before notifying affected participants, such as Plaintiffs and other Class members.

42. As noted above, the PII compromised in the Data Breach includes names,

[21] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.guanotronic.com/~serge/papers/weis07.pdf.

[22] *Id. at* n. 1, *supra*.

Social Security numbers, driver's license or state ID numbers, financial account and/or payment information.

43. Like Plaintiffs, other potential Class members received similar notices informing them that their PII was exposed in the Data Breach.

44. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures to protect its customers' and employees' PII, such as those it described in its June 2023 white paper.

D. FTC Guidelines Prohibit Eisner from Engaging in Unfair or Deceptive Acts or Practices.

45. Eisner is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

46. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[23]

47. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal

[23] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[24]

48. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[25]

49. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

50. Eisner failed to properly implement basic data security practices. Eisner's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

51. Eisner was at all times fully aware of its obligations to protect customers' and employees' PII, which gave it direct access to reams of customer and employee PII.

---

[24] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

[25] *Id.*

Defendant is also aware of the significant repercussions that would result from its failure to do so.

E. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

52. Cyberattacks and data breaches at companies that store PII are especially problematic because they can negatively impact on the overall daily lives of individuals affected by the attack.

53. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

54. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth,

[26] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

55. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

56. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[27]

57. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves,

[27] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed April 16, 2025).

and if they can get access to it, they will use it" to, among other things, open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

58. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

59. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[28]

60. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

61. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical

[28] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets." (citations omitted)).

fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs.

62. As discussed above, PII is a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

63. Social Security Numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [29]

64. For instance, with a stolen Social Security Number, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[30]

65. The Social Security Administration has warned that identity thieves can use

---

[29] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added).

[30] *Id.*

an individual's Social Security number to apply for additional credit lines.[31] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[32] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

66. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[33]

67. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Eisner is to get information that they can monetize by selling on the black market for

[31] *Id.*

[32] *Id.* at 4.

[33] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

68. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[34] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[35]

69. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*[36]

70. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years later. As with income tax returns, an individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notified the individual's employer of the suspected fraud.

---

[34] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[35] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[36] *Id.*

71. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[37]

72. Cybercriminals can post stolen PII on the cyber black-market for years following a data breach, thereby making such information publicly available.

73. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it happened.[38] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[39]

74. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[40]

75. It is within this context that Plaintiffs must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information

---

[37] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

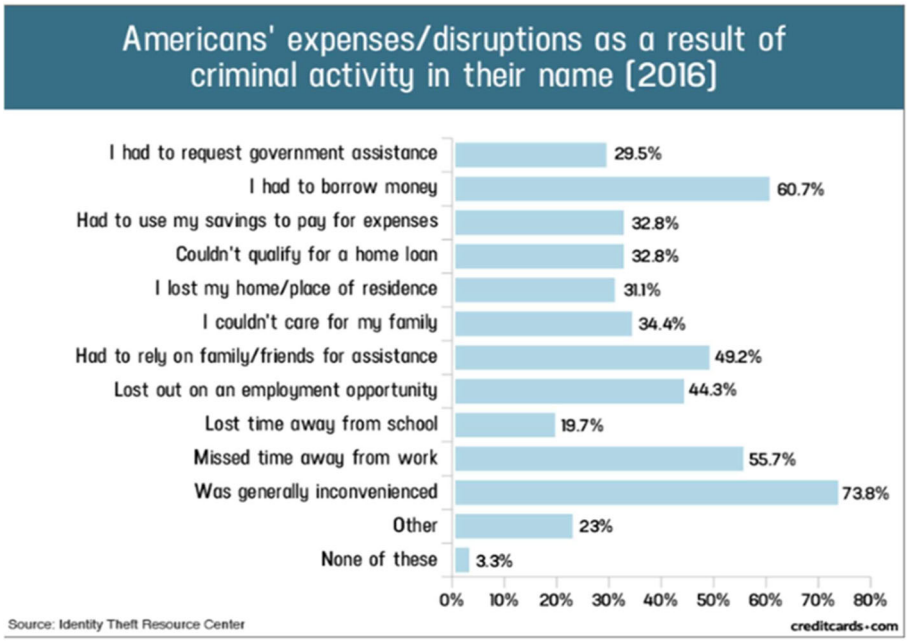
[38] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited April 16, 2025).

[39] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Apr. 17, 2023).

[40] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

for any number of improper purposes and scams, including making the information available for sale on the black market.

76. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.



77. Victims of the Data Breach, like Plaintiffs, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[41]

78. As a direct and proximate result of the Data Breach, Plaintiffs have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs must now take the time and effort (and spend the money) to mitigate the actual and potential

[41] *Id.*

impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing freezes and alerts with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

79. Moreover, Plaintiffs and Class members have an interest in ensuring that their PII, which remains in Eisner's possession, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Eisner has shown itself to be wholly incapable of protecting Plaintiffs' PII.

80. Plaintiffs and Class members also have an interest in ensuring that their personal information that was provided to Eisner is removed from Eisner's unencrypted files.

F. Plaintiffs and the Class Suffered Damages.

Facts Relevant to Plaintiffs

81. Eisner received Plaintiffs' PII in connection with its services. In maintaining Plaintiffs' PII for business purposes, Eisner expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiffs' and Class members' PII. Eisner did not, however, take proper care of Plaintiffs' and Class members' PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Eisner's inadequate security measures.

82. Plaintiffs received notice from Defendant notifying them that a security incident exposed their PII to criminals.

83. Upon receiving the Notice, Plaintiffs spent time reviewing their credit reports, reviewing various credit alerts received by text and email, checking their financial information, and dealing with increased spam text messages and emails.

84. Plaintiffs have suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from their PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiffs suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

85. Plaintiffs have experienced anxiety and increased concerns arising from the fact that their PII has been or will be misused and from the loss of their privacy.

86. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

87. Plaintiffs further suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that Plaintiffs entrusted to Defendant, which was compromised in and because of the Data Breach.

88. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

89. Plaintiffs have a continuing interest in ensuring that their PII which, upon information and belief, remains backed up in Defendant's possession, is protected and

safeguarded from future breaches.

Plaintiffs' And Class Members' Damages

90. For the reasons mentioned above, Eisner's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class members significant injuries and harm in several ways. Plaintiffs and Class members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiffs and Class members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

91. Once PII is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

92. As a result of Defendant's failures, Plaintiffs and Class members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII.

93. Further, because Defendant delayed in discovering and notifying Plaintiffs about the Data Breach, Plaintiffs were unable to take affirmative steps during that time

period to attempt to mitigate any harm or take prophylactic steps to protect against injury.

94. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[42] And identity fraud is only one of the harms victims face.

95. Plaintiffs are also at a continued risk because their information remains in Eisner's computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Eisner fails to undertake the necessary and appropriate security and training measures to protect its customers' and employees' PII.

96. In addition, Plaintiffs and Class members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ALLEGATIONS

97. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following class and subclass (collectively, the "Class"):

> **The Nationwide Class:** All individuals within the United States of America whose PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach experienced by Defendant including all who received a Notice of the Data Breach

[42] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited April 16, 2025).

> **The California Subclass:** All individuals residing in California whose PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach experienced by Defendant including all who received a Notice of the Data Breach

98. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

99. These proposed Class definitions are based on the information available to Plaintiffs at this time. Plaintiffs may modify the Class definitions in an amended pleading or when they move for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

100. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiffs are informed and believe, and thereon allege, that there are at minimum over one thousand members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Eisner's records, including but not limited to the files implicated in the Data Breach.

101. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Eisner had a duty to protect Plaintiffs' and Class members' PII;

b. Whether Eisner was negligent in collecting and storing Plaintiffs' and Class members' PII, and breached its duties thereby;

c. Whether Eisner breached its fiduciary duty to Plaintiffs and the Class;

d. Whether Eisner breached its duty of confidence to Plaintiffs and the Class;

e. Whether Eisner violated its own Privacy Practices;

f. Whether Eisner entered a contract implied in fact with Plaintiffs and the Class;

g. Whether Eisner breached that contract by failing to adequately safeguard Plaintiffs' and Class members' PII;

h. Whether Eisner was unjustly enriched;

i. Whether Plaintiffs and Class members are entitled to damages as a result of Eisner's wrongful conduct; and

j. Whether Plaintiffs and Class members are entitled to restitution as a result of Eisner's wrongful conduct.

102. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class all had information stored in Eisner's System, each having their PII exposed and/or accessed by an unauthorized third party.

103. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs are adequate representative of the Class because their interests do not conflict with the interests of the other Class members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex Class action litigation; Plaintiffs intend to prosecute

this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

104. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

105. **Superiority, Fed. R. Civ. P. 23(b)(3):** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Eisner. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

106. Eisner has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

107. Likewise, particular issues are appropriate for certification because such

claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Eisner failed to timely and adequately notify the public of the Data Breach;

b. Whether Eisner owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Eisner's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Eisner's failure to institute adequate protective security measures amounted to negligence;

e. Whether Eisner failed to take commercially reasonable steps to safeguard consumers' and employees' PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

108. Finally, all members of the proposed Class are readily ascertainable. Eisner has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST CAUSE OF ACTION
NEGLIGENCE
(Plaintiffs on behalf of the Nationwide Class)

109. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

110. Plaintiffs bring this claim individually and on behalf of the Class.

111. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, and control.

112. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

113. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

114. Defendant breached the duties owed to Plaintiffs and Class members and thus was negligent. As a result of a successful attack directed to Defendant that compromised Plaintiffs' and Class members' PII, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur:

(a) mismanaging its system and failing to identify reasonably foreseeable internal

and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

115. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, their PII would not have been compromised.

116. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following

fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of

attacks on Plaintiffs and Class members.

117. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(Plaintiffs on behalf of the Nationwide Class)

118. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

119. Plaintiffs bring this claim individually and on behalf of the Class.

120. Upon information and belief, Defendant entered into contracts with its corporate customers to provide services that included data security practices, procedures, and protocols sufficient to safeguard the PII that was entrusted to it.

121. Such contracts were made expressly for Plaintiffs' and the Class' benefit as it was their PII that Defendant agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

122. Defendant knew or should have known that if it were to breach these contracts with its customers, Plaintiffs and Class Members would be harmed.

123. Defendant breached its contracts with corporate customers by, among other things, failing to adequately secure Plaintiffs and Class Members' PII, and, as a result, Plaintiffs and Class Members were harmed by Defendant's failure to secure their PII.

124. As a direct and proximate result of Defendant's breach, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their PII; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their PII, which remains in Defendant's control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

125. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

126. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(Plaintiffs on behalf of the Nationwide Class)

127. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

128. Plaintiffs and Class members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

129. As a recipient of consumers' PII, Defendant has a fiduciary relationship to Plaintiffs and the Class members.

130. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable PII related to Plaintiffs and the Class. Plaintiffs and the Class were entitled to expect their information would remain confidential while in Defendant's possession.

131. Defendant owed a fiduciary duty under common law to Plaintiffs and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

132. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiffs' and the Class members' records.

133. Defendant had possession and knowledge of confidential PII of Plaintiffs and Class members, information not generally known.

134. Plaintiffs and Class members did not consent to nor authorize Defendant to release or disclose their PII to unknown criminal actors.

135. Defendant breached its fiduciary duties owed to Plaintiffs and Class members by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its customers and employees; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

136. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiffs and Class members, their PII would not have been compromised.

137. As a direct and proximate result of Defendant's negligence, Plaintiffs and

Class members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

138. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(Plaintiffs on behalf of the Nationwide Class)

139. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

140. Plaintiffs and Class Member have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

141. Plaintiffs and Class members provided Defendant with their personal and confidential PII under both the express and/or implied agreement of Defendant to limit the use and disclosure of such PII.

142. Defendant owed a duty to Plaintiffs and Class members to exercise the

utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

143. Plaintiffs' and Class members' PII is not generally known to the public and is confidential by nature.

144. Plaintiffs and Class members did not consent to nor authorize Defendant to release or disclose their PII to an unknown criminal actor.

145. Defendant breached the duties of confidence it owed to Plaintiffs and Class members when their PII were disclosed to unknown criminal hackers.

146. Defendant breached its duties of confidence by failing to safeguard Plaintiffs' and Class members' PII, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; (h) storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of

Plaintiffs' and Class members' PII to a criminal third party.

147. But for Defendant's wrongful breach of its duty of confidences owed to Plaintiffs and Class members, their privacy, confidences, and PII would not have been compromised.

148. As a direct and proximate result of Defendant's breach of Plaintiffs' and Class members' confidences, Plaintiffs and Class members have suffered injuries, including:

a. The erosion of the essential and confidential relationship between Defendant and Plaintiffs and Class members as parties that were subject to the business relationship;

b. Theft of their PII;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Eisner Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services,

freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and

j. Loss of personal time spent carefully reviewing financial and medical statements to check for charges for services not received.

149. Defendant breached the confidence of Plaintiffs and Class members when it made an unauthorized release and disclosure of their confidential information and, accordingly, it would be inequitable for Defendant to retain the benefit at Plaintiffs' and Class members' expense.

150. As a direct and proximate result of Defendant's breach of its duty of confidences, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an

amount to be proven at trial.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiffs on behalf of the Nationwide Class)

151. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

152. Plaintiffs brings this claim individually and on behalf of the Class.

153. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class members.

154. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

155. Plaintiffs and Class members conferred a monetary benefit on Defendant. In exchange, Plaintiffs and Class members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

156. Defendant knew that Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class members for business purposes.

157. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members'

PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

158. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

159. Defendant failed to secure Plaintiffs and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class members provided.

160. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

161. If Plaintiffs and Class members knew that Defendant had not reasonably secured their PII, they would not have agreed to have their information provided to Defendant.

162. Plaintiffs and Class members have no adequate remedy at law.

163. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

164. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

165. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class members overpaid for Defendant's accounting and tax advisory services.

SIXTH CAUSE OF ACTION
CALIFORNIA CONSUMER PRIVACY ACT, CALIFORNIA CIVIL CODE § 1798.100
(Plaintiff Christ on behalf of the California Subclass)

166. Plaintiff restates and realleges the preceding allegations in the paragraphs above as if fully alleged herein.

167. Plaintiff and California Subclass Members are "consumer[s]" as that term is defined in Cal. Civ. Code § 1798.140(g) because they are natural persons and California residents.

168. Defendant is a "business" as that term is defined in Cal. Civ. Code § 1798.140(c) because, on information and belief, it has annual gross revenue exceeding $25 million and it buys, receives, sells, and shares personal information of 50,000 or more

consumers, households, or devices.

169. The Plaintiff's and Class Members' PII is "nonencrypted and nonredacted personal information" consisting of social security number, names, addresses and other sensitive personal information. Cal. Civ. Code § 1798.150(a)(1). The Data Breach constitutes "an unauthorized access and exfiltration, theft, or disclosure" pursuant to Cal. Civ. Code § 1798.150(a)(1) because due to Defendants' failure to implement reasonable and necessary security measures, they enabled third party criminals to access personal information and thus, caused unauthorized sharing of Plaintiff's and the Class Members' personal information.

170. Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of Plaintiff's and Class Members' PII to protect said PII.

171. Defendant breached the duty they owed to Plaintiff and Class Members described above. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of the Plaintiff and Class Members; (b) detect the breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

172. Defendants breach of the duty they owed to Plaintiff and the Class Members described above was the direct and proximate cause of the Data Breach. As a result, Plaintiff and the Class Members suffered damages, as described above and as will be proven at trial

173. Plaintiff and the Class Members seek injunctive relief in the form of an order

enjoining the Defendants from continuing the practices that constituted their breach of the duty owed to Plaintiff and Class Members as described above.

SEVENTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiffs on behalf of the Class)

174. Plaintiffs restate and reallege the preceding allegations in the paragraphs above as if fully alleged herein.

175. Plaintiffs bring this claim individually and on behalf of the Class.

176. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

177. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their PII. Plaintiffs and the Class remain at imminent risk that additional compromises of their PII will occur in the future.

178. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

179. Defendant still possess Plaintiffs' and Class members' PII.

180. Defendant has made no announcement that it has changed its data storage or security practices relating to the storage of Plaintiffs' and Class members' PII.

181. To Plaintiffs' knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

182. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Eisner. The risk of another such breach is real, immediate, and substantial.

183. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Eisner, Plaintiffs and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

184. Issuance of the requested injunction will not compromise the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Eisner, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other consumers whose PII would be further compromised.

185. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Eisner implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Eisner's systems on a periodic basis, and ordering Eisner to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying PII not necessary for its provisions of accounting and tax advisory services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b. For equitable relief enjoining Eisner from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs'

and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

c. For equitable relief compelling Eisner to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Eisner's wrongful conduct;

e. Ordering Eisner to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and,

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded by Plaintiffs on all claims so triable.

Dated: April 17, 2025

Respectfully submitted,

/s/David A. Goodwin
Daniel E. Gustafson
David A. Goodwin

Joshua J. Rissman
Joe E. Nelson
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South 6th Street, Suite 2600
Minneapolis, MN 55402
Telephone: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com
jrissman@gustafsongluek.com
jnelson@gustafsongluek.com

Marc H. Edelson (*pro hac vice forthcoming*)
Liberato P. Verderame (*pro hac vice forthcoming*)
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
Telephone: (215) 867-2399
medelson@edelson-law.com
lverderame@edelson-law.com

Attorneys for Plaintiffs and the Putative Class